UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the email account gradengretch@gmail.com

Case No. 14-M-217

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A2

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B2

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United State Code, Sections 1030(a)(5)(A) and 2	fraud and related activity in connection with computers and aiding and abetting fraud and related activity in connection with computers.

The application is based on these facts:

☑ Continued on the attached sheet.

☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Eliot J. Mustell, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: February 14, 2014

Judge's signature

City and state: Milwaukee, Wisconsin

Patricia J. Gorence, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT)
) ss
EASTERN DISTRICT OF WISCONSIN)

AFFIDAVIT

I, Eliot J. Mustell, being duly sworn and under oath state the following:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been employed with the FBI since February 2013. I am currently assigned to the FBI Milwaukee Division's Cyber Crimes Task Force. Prior to becoming a Special Agent with the FBI, I worked in a variety of private positions in the Information Technology industry.

2. As a Special Agent with the FBI, I investigate criminal and national security related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of SPAM, malicious software, the theft of identification information, and other computer-based fraud. Since joining the FBI, I have been involved in numerous criminal and national security investigations involving computer intrusions. I have received training in computer technology, and computer-based fraud; and I have held industry certification from Cisco, EC Council, and Microsoft.

3. This affidavit is made in support of an application for a search warrants under 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Google, Inc., ("Google") to disclose to the United States copies of the information stored at premises owned, maintained, controlled, or operated by Google, an e-mail provider headquartered at Google Legal Investigations Support, 1600 Amphitheatre Parkway, Mountain View, California, 94043, including the content of communications, further described in Section I of Attachments B1 and B2, associated with the following email accounts: (a) Google email account xtreme.hf2@gmail.com; and (b) Google email account gradengretch@gmail.com. The information to be searched is described below and in Attachments A1 and A2. Upon receipt of

the information described in Section I of Attachments B1 and B2, government-authorized persons will review that information to locate the items described in Section II of Attachments B1 and B2.

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth facts that I believe are sufficient to establish probable cause to believe that an unknown individual or individuals have committed violations of Title 18, United States Code, Sections 1030(a)(5)(A) and 2 (fraud and related activity in connection with computers and aiding and abetting fraud and related activity in connection with computers); and that evidence and instrumentalities concerning those violations will be found in the information, including the content of communications, further described in Attachments B1 and B2, associated with email accounts: xtreme.hf2@gmail.com, gradengretch@gmail.com.

DEFINITIONS

5. Based on my training and experience, I know the following:

a. The Internet is a global network of computer systems that allow individual computers to communicate through a set of established protocols. For the purposes of this Complaint, a computer is defined as a device, including computers, routers, switches, smart phones, portable digital assistants, game consoles, etc. that has the ability to communicate with another device over the Internet utilizing the TCP/IP protocol. In order to communicate effectively, these devices are assigned a unique identifier known as an Internet Protocol (IP)

address. Every device connected to the Internet has an assigned unique IP address that allows it to communicate with other device.

b. A "bot" is a computer that contains a software program that interacts with network services intended for people as if it were a person. The term is derived from the word "robot." There are both illegal and legal uses for a bot. However, in this investigation, a bot is malicious in that it is used to send and receive commands on computers that have been accessed without authorization.

c. A "botnet" is a collection of software robots, or bots, which run autonomously. The term is derived from "robot network." The term "botnet" is generally used to refer to a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure. A botnet's originator, also known as a "bot-herder" can control the group remotely through various means and usually for nefarious purposes. Botnets serve various criminal purposes, including launching and controlling denial-of-service attacks, creating and misusing Simple Mail Transfer Protocols mail relays or proxies for spam, click fraud, and the theft of identification information.

d. "Bullet proof hosting" is a term used for a web hosting provider that will host virtually any content, from phishing and carding sites to botnet command centers and Internet browser exploit kits.

e. Phishing is an attempt to obtain financial or other confidential information from Internet users, typically by sending an e-mail that looks as if it is from a legitimate organization (frequently a financial institution), but which contains a link to a fake Web site that replicates the real one. The e-mail is typically referred to as "SPAM."

f. Internet Relay Chat ("IRC") is an instant messaging computer network used for group communication that allows a user to chat online in real time with other users through various IRC client applications structured in a client-server model. IRC allows user to communicate, share with other IRC channels all around the world. IRC setup involves a central point for clients to connect in order to relay text based communication. Users can use IRC in either a multi-user group conference or in a one-to-one private discussion known as Direct Client to Client ("DCC") communication. DCC still uses the original IRC orientated protocol, but once the connection is established through the IRC server the two clients communicate directly with one another bypassing the central server.

g. A Distributed Denial of Service ("DDOS")[1] is a type of attack that prevents authorized users from processing incoming information. Multitudes of compromised computers flood the target with incoming messages. The goal of a DDOS attack is to keep the processing or attacked unit busy with spurious tasks. The incoming messages resulting from a DDOS attack essentially saturate the targeted machine with external communication requests until it cripples the targeted machine and the targeted machine is unable to respond to any legitimate traffic.

[1]DDOS attacks can cause a business to suffer enormous financial losses. According to a survey companies in 2012 by neustar.biz, the potential financial loss from a successful DDOS attack would be $10,000 per hour. According to enzinemark.com, the cost of a company's proactive protections from a DDOS attack is approximately $300,000 annually.

PROBABLE CAUSE[2]

6. On or about November 4, 2013, a confidential source of information ("CS-1")[3] informed the FBI that he/she had located multiple advertisements offering computer hacking utilities for sale on an Internet forum frequented by computer hackers.[4] According to information associated with the advertisements, the advertisements were posted by an individual using on the alias "Remarkable." For example, the following advertisement was posted by Remarkable on the Internet forum on or about October 7, 2013:

> We have a new service that we would like to offer this forum we have started to sell high quality root. What are roots they are hacked Linux servers that you can do what you wish with them, you also have full access to the serve (sic). Our roots have great uptime [the hacked servers are reliable and are up for long periods of time] and they are also cheap and stable. Contact Skype - xtreme.HF Email – Xtreme.HF2@gmail.com [an interested party could contact Remarkable through Skyp at xtreme.HF or through email at Xtreme.HF2@gmail.com]

7. On or about November 1, 2013, based on the above described advertisement, CS-1 consensually recorded an instant message exchange with Remarkable using Skye, who was

---

[2] At various points in this affidavit, I will offer my interpretation of certain conversations and the meaning to certain terms in brackets. My interpretation of these conversations is based on my knowledge of the investigation to date, conversations with other law enforcement officers and agents, conversations with a confidential source of information, and my experience and familiarity with these types of investigations. The summaries of conversations do not include all potentially criminal conversations during this investigation, or all statements or topics covered during the course of the conversation. All quoted conversations in this this affidavit do not represent finalized transcripts and may not represent the entire conversation that occurred between the identified individuals.

[3] CS-1 has been cooperating with law enforcement on this investigation since in or around September 2011. CS-1 has a prior federal conviction. CS-1 is cooperating with law enforcement as part of his/her plea agreement with the United States. CS-1 is also cooperating in exchange for immigration and financial benefits. CS-1 has provided law enforcement with timely and accurate information corroborated by law enforcement through consensually recorded conversations, controlled buys, and law enforcement reporting.

[4] According to CS-1, a self-admitted computer hacker, the advertisements were on an Internet forum CS-1 knows to be frequented by individuals involved in the unauthorized access of third-party computers.

using Skype account xtreme.HF.[5] According to the instant message exchange between xtreme.HF and CS-1, in addition to compromised roots, CS-1 indicated that he/she was interested in buying bots to conduct DDOS attacks. In response, xtreme.HF advised CS-1 that xtreme.HF could provide access to an IRC-based DDOS botnet with full control of the bots for DDOS attacks. According to xtreme.HF, the botnet is maintained by xtreme.HF; and it can conduct a DDOS attack with 10-14 gbps of bandwidth.[6] Xtreme.HF also indicated that the botnet allow for unlimited amount of boot times. Based on my training and experience, I know that an unlimited amount of boot times means that a user could continuously use the botnet for an unlimited amount of DDOS attacks during the month that the botnet is leased.

8. On or about November 4, 2013 CS-1 consensually recorded an instant message exchange with xtreme.HF over Skype. During the instant message exchange, xtreme.HF agreed to rent the use of the botnet for one month for $200. Xtreme.HF directed CS-1 send the $200 to WebMoney account Z338809391625. A short time later, law enforcement agents transferred $200 to WebMoney account Z338809391625, as directed by xtreme.HF, in exchange for access to the botnet. When transferring the money to the WebMoney account, a limited account holder profile was available for agents to view. According to the WebMoney profile viewable at the

---

[5]The individual using the online monikers "Remarkable" and "xtreme.HF" has not yet been fully identified. For purpose of this affidavit, that individual is referred to by the name "xtreme.HF" and is considered to be a male.

[6]Xtreme.HF was indicating that the botnet can conduct a DDOS attack with the bandwidth throughput of 10-14 gigabits per second. That means that if the target of the DDOS attack has bandwidth equal or less than 10-14 gbps the target of the attack will be completely disabled by the attack. In case where a victim has slightly greater bandwidth than the attacker the victim will still be significantly impaired by this attack. Bandwidth represents the rate at which a network can operate. Based on my training and experience I know the typical average bandwidth at which an individual accesses the Internet is 8.6 megabits per second. I know that 1 gigabit is equal to 1000 megabits.

time of the money transfer to account Z338809391625, Google email address gradengretch@gmail.com was associated with the account.

9. On or about November 5, 2013, CS-1 consensually recorded an instant message exchange with xtreme.HF over Skype. During the instant message exchange, xtreme.HF directed CS-1 to install a client IRC application called "mIRC." Once installed, mIRC allowed agents to control and communicate with the bot-herder IRC server, which then allowed agents to control the bots comprising the botnet through a series of command described below. After agents installed the client application mIRC, xtreme.HF provided the bot-herder IP address (89.248.172.144) to CS-1.[7] Xtreme.HF then sent the series of attack commands listed below to CS-1:

a. verify – [to verify yourself to the bots, which allows the user to begin controlling the bots through IRC]

b. shellcmd ./v ip port ip (ip in this command is written twice) – [used to initiate DDOS attack on the identified IP address]

c. shellcmd ./stealth ip port [ensured the bot sending out traffic for the DDOS attack would not respond to any responsive incoming communications, which allowed the bot to be available for a DDOS attack]

d. stopcmd – [used to stop a DDOS attack]

Based on my training and experience and conversations with other experienced agents and officers, I believe that the command structure listed above indicates that xtreme.HF is using a command line denial of service utility to operate the botnet.

10. On or about December 5, 2013, CS-1 had a consensually recorded instant message exchange with xtreme.HF over Skype. During the instant message exchange,

[7] An open source query of IP address 89.248.172.144 using Whois look up, revealed that the bot-herder server was located in the Netherlands. The location of the bot-herder server has since. Whois is a widely-used Internet protocol that lists contact and registry information for a domain name and IP address.

xtreme.HF told CS-1 that CS-1 should upgrade to a new botnet package for $350 per month that would allow CS-1 to conduct DDOS attacks three times more powerful than the DDOS attack current available to CS-1 through the botnet. Agents did not buy access to new botnet package. Later on during the same instant message exchange, CS-1 asked xtreme.HF whether other individuals who wanted to rent the botnet should be referred to xtreme.HF or Remarkable (the individual responsible for posting the advertisement described in paragraph 6). In response, xtreme.HF stated that other potential customers should contact him at xtreme.HF using Skype because Remarkable was just another online moniker that he used.

11. On or about December 16, 2013, CS-1 had a consensually recorded instant message exchange with xtreme.HF over Skype. During the exchange, xtreme.HF indicated that CS-1's access to the botnet had expired, but stated CS-1's monthly access to the botnet could be renewed for $160. A short time later, law enforcement agents transferred $160 to WebMoney account Z185473367543.

12. Based on a FBI analysis of the botnet rented from xtreme.HF, I determined that xtreme.HF's botnet is comprised of approximately 100 bots. Based on my training and experience, and conversation with other law enforcement agents and officers, I believe that each of the approximately 100 bots represents a computer that has been accessed without authorization and infected with malware or a worm for the purpose of using that computer as part of a botnet. Based on the IP addresses for those bots and a Whois query of those IP addresses, I learned that seven of the bots are located in the United States. The bots in the United Sates consisted primarily of virtual private servers, which are servers owned by cloud-based server hosting companies who lease servers to third parties.

13. At the time of the analysis discussed in the preceding paragraph, the FBI determined that the IP address for the bot-herder was 209.20.66.191. According to a Whois query, that IP address resolves to a server owned and operated by Rackspace, a cloud-based server hosting company located in the United States. According to information obtained from Rackspace, during the time period relevant to this investigation, the server associated with IP address 209.20.66.191was being leased to Victim Company A. According to a representative from Rackspace, in July and September of 2013, Rackspace received complaints from Victim Company B and Victim Company C, who indicated that they had both been the subject of an IRC DDOS attack, which Victim Company B and Victim Company C traced to IP address 209.20.66.191.[8] Based on my training and experience, and conversation with other law enforcement agents and officers, and conversations with representatives from Rackspace, I believe that xtreme.HF accessed the Rackspace server leased to Victim Company A without authorization and used the server as the bot-herder. Additionally, I believe that xtreme.HF or one of his botnet customers executed a DDOS attack on the networks of Victim Company B and Victim Company C using xtreme.HF's botnet.

14. On or about November 6, 2013, a Grand Jury Subpoena was issued to Google for information related to the email address xtreme.hf2@gmail.com, which was the email address listed in the advertisement described above in paragraph 6. According to records obtained from Google, email address xtreme.hf2@gmail.com was registered on August 4, 2013, from IP address 85.159.233.115. According to a Whois query, IP address 85.159.233.115 resolves to an

[8]Victim Company B and Victim Company C are based outside the United States; and the FBI has not yet interviewed a representative from either company. The extent of the damage caused by the DDOS attack has not yet been determined.

open proxy server.[9] Based on my training and experience, I know that individuals committing criminal conduct over the Internet often use proxy servers to conceal their identities.

15. On or about November 6, 2013, a Grand Jury Subpoena was issued to Google for account information related to email account gradengretch@gmail.com, which was the email account associated with the WebMoney account Z338809391625, as described above in paragraph 8. According to records obtained from Google, email address gradengretch@gmail.com was registered on February 27, 2013, from IP address 69.65.47.126. According to a Whois query, IP address 69.65.47.126 resolves to an open proxy server called openVPN.net.

16. On January 23, 2014, United States Magistrate Judge Nancy Joseph issued orders authorizing the installation and use of a pen register and trap and trace device or process on email accounts xtreme.hf2@gmail.com and gradengretch@gmail.com ("1/23/2014 pen-trap orders"). Based on the information obtained from the 1/23/2014 pen-trap orders, I know that Gmail account xtreme.hf2@gmail.com has received emails from services such as noreply@hidemyass.com. Based on my experience and open source information, I know hidemyass.com is a proxy used to conceal the user's IP address. Gmail account gradengretch@gmail.com received numerous emails from billing@sh3lls.net. According to open source information, sh3lls.net is a cloud-based server hosting business. In addition, gradengretch@gmail.com received emails from Ecatel@bill.info. According to open source

[9] A proxy server is a computer system that acts as an intermediary between an end-user and the destination such as a website as a way obfuscate the originating location of the end-user. This means the destination location would only see the proxy server's IP address and not an end-user's IP address, which in certain cases could be the end-user's home network. This would also mean the end-user's destination would be shown only as the proxy server instead of the actual website visited. Based on my training and experience, and conversations with other experienced agents, I believe that the primary purpose of using a proxy server to register Google email address xtreme.hf2@gmail.com was to conceal the end-user's IP address. This means the destination location would only see the proxy server's IP address not the users IP address.

information, Ecatel is a Netherlands based cloud-based server hosting business. Based on my training and experience, I believe that the emails described above are consistent with an individual actively purchasing server hosting in an attempt to host sites or to act as a proxy to conceal their originating IP address, which is consistent with the criminal activity associated with operating the botnet under investigation in this case.

DELAYED NOTIFICATION

17. The search warrants in this case are being sought in a covert ongoing investigation. The investigation will continue beyond the date on which the sought after search warrants are executed. Certain evidence, like the materials sought in the search warrant for the Google email accounts, is stored electronically and can be accessed and deleted remotely. Therefore, notifying the subscriber of the execution of the search warrants at Google would likely cause adverse results, including flight from prosecution, destruction or tampering with evidence, and otherwise seriously jeopardize the investigation. *See* 18 U.S.C. § 2705(b)(2), (3), (5). Therefore, the government asks that notice of the execution of the search warrants be delayed for at least 30 days.

BACKGROUND CONCERNING E-MAIL

18. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Google allows subscribers to obtain free e-mail accounts at the domain name gmail.com like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers

and their use of Google services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

20. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage

of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

22. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

CONCLUSION

23. Based on the information stated above, I respectfully submit that probable cause exists to believe that violations of Title 18, United States Code, Sections 1030 and 2 have been committed and evidence and instrumentalities concerning those violations will be found in information, including the content of communications, further described in Section I of Attachments B1 and B2, associated with email accounts: xtreme.hf2@gmail.com and gradengretch@gmail.com, which information is stored at premises owned, maintained, controlled, or operated by Google, Inc., an e-mail provider headquartered at Google Legal Investigations Support, 1600 Amphitheatre Parkway, Mountain View, California, 94043, as described in Attachment A1 and A2.

ATTACHMENT A2

Property to Be Searched

Information associated with gradengretch@gmail.com that is stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheater Parkway, Mountain View, California, 94043.

ATTACHMENT B2

Particular Things to be seized

II. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment B2 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on March 15, 2013, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A2:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, deleted emails, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including Web history, address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. §§ 1030(a)(5)(A) and 2 involving gradengretch@gmail.com, including information pertaining to the following matters:

a. Communications and websites related to the registration of Internet domains.

b. Communications and websites related to malware and/or computer viruses.

c. Communications websites related to computer botnets.

d. Communications and websites related to financial transactions.

e. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.